HiPER 命令行配置手册

第 5 卷：NAT 配置

上海艾泰科技有限公司

http://www.utt.com.cn

版 权 声 明

版权所有©2000-2005，上海艾泰科技有限公司，保留所有权利。

本文档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本文档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

遵守所生效的版权法是用户的责任。在未经上海艾泰科技有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

上海艾泰科技有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经艾泰科技有限公司明确书面许可的情况下，使用本文档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰®、UTT®文字及相关图形是上海艾泰科技有限公司的注册商标。

HiPER®文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0900-0045-001

文档编号（DN）：PR-PMMU-1106.06-PPR-CN-1.0A

目 录

导 读 1

第 1 章 NAT 基本概念 2

1.1 NAT 概述......2
1.2 NAT 的基本类型......2
1.2.1 基本 NAT......2
1.2.2 NAPT 3

第 2 章 HIPER 中 NAT 的实现......5

2.1 相关术语......5
2.2 NAT 功能介绍......5
2.2.1 概述......5
2.2.2 NAT 地址空间......6
2.2.3 三种 NAT 类型......6
2.2.4 主线路 NAT 规则和备份线路 NAT 规则 6
2.2.5 根据源地址指定优先通道......7
2.2.6 根据线路带宽合理分配线路流量......7
2.2.7 两种流量分配规则......7
2.2.8 NAT 静态映射......8
2.2.9 虚拟服务器（DMZ 主机） 8
2.2.10 NAT 规则的执行顺序......9
2.3 NAT 转换表（NAT 会话表） 9
2.3.1 概述......9
2.3.2 NAT 转换表项（NAT 会话）的类型 9
2.3.3 动态生成的 NAT 会话......10
2.3.4 使用 NAT 静态映射生成的 NAT 会话 10
2.4 NAT ALG 功能......10

第 3 章 NAT 配置 12

3.1 NAT 全局配置......12
3.1.1 启用/禁用 NAT 功能......12
3.1.2 设置最大 session 数 12
3.1.3 设置分配规则......13
3.2 NAT 规则配置......13
3.2.1 NAT 规则配置——EasyIP 类型......13
3.2.1.1 新建一条 NAT 规则 14
3.2.1.2 设置 NAT 规则的类型为 EasyIP......14
3.2.1.3 设置外部 IP 地址 14
3.2.1.4 设置内部起始 IP 地址和内部结束 IP 地址......15
3.2.1.5 设置权重......15

3.2.1.6 设置绑定线路（端口）......15
3.2.1.7 启用/禁用一条 NAT 规则......16
3.2.1.8 删除一条 NAT 规则......16
3.2.2 NAT 规则配置——One2One 类型......16
3.2.2.1 新建一条 NAT 规则......16
3.2.2.2 设置 NAT 规则的类型为 One2One......17
3.2.2.3 设置外部起始 IP 地址......17
3.2.2.4 设置内部起始 IP 地址和内部结束 IP 地址......17
3.2.2.5 设置绑定线路（端口）......18
3.2.2.6 启用/禁用一条 NAT 规则......18
3.2.2.7 删除一条 NAT 规则......19
3.2.3 NAT 规则配置——Passthrough 类型......19
3.2.3.1 新建一条 NAT 规则......19
3.2.3.2 设置 NAT 规则的类型为 Passthrough......19
3.2.3.3 设置内部起始 IP 地址和内部结束 IP 地址......20
3.2.3.4 设置绑定线路（端口）......20
3.2.3.5 启用/禁用一条 NAT 规则......20
3.2.3.6 删除一条 NAT 规则......21
3.3 NAT 静态映射配置......21
3.3.1 新建一条 NAT 静态映射......21
3.3.2 设置协议类型......22
3.3.3 设置内部 IP 地址......22
3.3.4 设置内部起始端口......22
3.3.5 设置外部起始端口......23
3.3.6 设置端口浮动范围......23
3.3.7 设置绑定的 NAT 规则......23
3.3.8 启用/禁用一条 NAT 静态映射......24
3.3.9 删除一条 NAT 静态映射......24
3.4 DMZ 主机的配置......24
3.4.1 设置全局 DMZ 主机......24
3.4.2 设置局部 DMZ 主机......25
3.5 NAT 配置的注意事项......25
3.6 NAT 的显示和诊断......26
3.6.1 查看 NAT 摘要信息......26
3.6.2 查看 NAT 会话表......28
3.6.3 查看 NAT 静态映射......29
3.6.4 局域网各主机的 NAT 统计信息的查看和清除......30
第 4 章 NAT 配置实例......32
4.1 NAT 规则配置实例......32
4.1.1 EasyIP 方式应用实例......32
4.1.2 One2One 方式应用实例......34
4.1.3 Passthrough 方式应用实例......37
4.2 NAT 静态映射配置实例......39
4.2.1 NAT 静态映射配置实例 1......39

4.2.2 NAT 静态映射配置实例 2 40
4.2.3 NAT 静态映射配置实例 3 41

附录一 图目录 42

附录二 表目录 43

导　　读

命令行格式约定

本手册中，讲解命令句法时，英文字体为“ Times New Roman ”字体，中文字体为“ 宋体 ”。相关命令行格式约定的描述如下：

加粗字体：指配置命令时需要原封不动输入的参数。

倾斜字体：指配置命令时必须为之提供实际值的参数。

[ ]：表示用[ ]扩起来的部分，在配置命令时是可选的。

{x | y | … }：表示从两个或多个选项中选取一个。

[x | y | …]：表示从两个或多个选项中选取一个或者不选。

！：由感叹号！开始的行表示注释行。

_ ：输入光标位置。

>:命令行参数层次分隔符。

此外，在实际的配置实例和终端输出（Terminal Display）中，使用加粗“ Courier New ”字体表示用户从终端输入的信息；使用普通“ Courier New ”字体表示屏幕输出信息。

键盘操作约定

<>：表示键盘上的按键。例如，<Enter>表示回车。

<键 1+键 2>：表示在键盘上同时按下键 1 和键 2。例如，<Ctrl+H>表示同时按下 Ctrl 键和 H 键。

特殊符号约定

该符号表示提示信息，指出重点注意事项。

适用版本

本手册适用的软件版本为 ReOS 5.0。

第1章 NAT 基本概念

1.1 NAT 概述

NAT（Network Address Translation）是一种将一个 IP 地址域（如 Intranet）映射到另一个 IP 地址域（如 Internet）的技术。NAT 的出现是为了解决 IP 日益短缺的问题，将多个内部地址映射为少数几个甚至一个公网地址。这样，就可以实现内部网络中的主机（使用私有地址）透明的访问外部网络中的资源；同时，外部网络中的主机也可以有选择的访问内部网络。而且，NAT 能使得内外网络隔离，提供一定的网络安全保障。

NAT 功能通常被集成到路由器、防火墙、网关等或者单独的 NAT 设备中。这些提供 NAT 功能的设备均维护一个 NAT 转换表,用来记录地址转换或者地址端口转换的相关信息。

注意，内部地址是指局域网内部主机使用的 IP 地址；公网地址是指在 Internet 上全球唯一的合法 IP 地址。一般情况下，建议内部地址使用 RFC1918 规定的私有地址。RFC1918 为私有网络预留出了三个 IP 地址块，具体如下：

- A 类：10.0.0.0～10.255.255.255
- B 类：172.16.0.0~172.31.255.255
- C 类：192.168.0.0～192.168.255.255

由于上述三个范围的地址专门提供给私有网络，不会在 Internet 中被分配使用的，因而可以在公司内部自由使用。公司或企业可以根据内部网络的规模大小采用私有地址网段分配给内部网络，满足内部网络互连的需求。

1.2 NAT 的基本类型

传统 NAT 按功能可以分为基本 NAT 和 NAPT（即网络地址端口转换）两大类，有关传统 NAT 的详细描述请参见 RFC1631 和 RFC3022。另外，在 NAT 技术领域，还实现了双向 NAT（Bi-directional NAT）、两次 NAT(Twice NAT)、多宿主 NAT（Multihomed NAT）等类型的 NAT。本手册主要介绍传统 NAT，即基本 NAT 和 NAPT。

1.2.1 基本 NAT

基本 NAT 将内部地址与合法公网地址进行一对一的转换，根据其实现方式不同，又分为静态 NAT 和动态 NAT 两类。静态 NAT 中，内部网络中的每个主机都被永久地映射成外部网络中某个合法的地址。而动态 NAT 则是在网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。

基本 NAT 只是转换 IP 地址，当位于内部网络中的主机通过 NAT 设备向外部主机发起会话请求时，NAT 设备就会查询 NAT 表，看是否有相关会话记录，如果有相关记录，就会将内部 IP 地址转换成合法公网地址，再转发出去；如果没有相关记录，进行地址转换的同时，还会在 NAT 表增加一条该会话的记录。外部主机接收到数据包后，用接受到的合法公

网地址作为目的 IP 地址来响应，NAT 设备接收到外部回来的数据包，再根据 NAT 表把目的 IP 地址转换成对应的内部 IP 地址，转发给该内部主机。一个内部主机可以使用相同的地址转换同时发起多个会话。

以下给出了一个实例（如图 1-1），并通过该实例详细地描述了网络地址转换（基本 NAT）的基本过程。

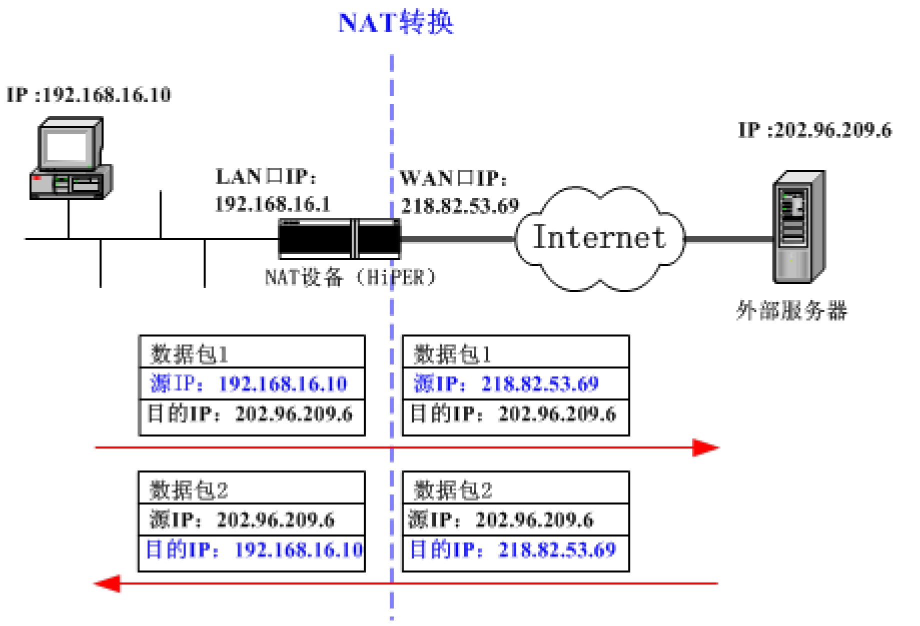

图 1-1 网络地址转换（基本 NAT）的基本过程

图 1-1 中，通过具有 NAT 功能的 NAT 设备（这里以 HiPER 为例说明）来连接内部局域网和公有网络。当内部 PC 向（IP 为 192.168.16.10）向外部服务器（IP 为 202.96.209.6）发送一个请求数据包 1（初始源 IP 为 192.168.16.10）时，该数据包将通过 HiPER 来转发。HiPER 接收到数据包 1 后，先通过 NAT 将其源 IP 转换为 218.82.53.69，然后再转发该数据包；同时，在 NAT 映射表中，将增加（或刷新）一条相关记录。外部服务器收到数据包 1 后，就给内部 PC 发送一个回复数据包 2（初始目的 IP 为 218.82.53.69），当 HiPER 接收到数据包 2 后，首先查找 NAT 映射表中相关记录，然后用原来的 PC 机内部 IP 地址 192.168.16.10 替换目的 IP 地址 218.82.53.69，最后再将数据包 2 转发给该 PC 机。

显然，上述的 NAT 过程对于终端（内部 PC 机和外部服务器）是透明的。对于外部服务器来说，它认为内部 PC 机的地址就是 218.82.53.69，并不知道 192.168.16.10 的存在。因此，可以说 NAT 有效地隐藏了企业的内部局域网。

如果内部网络中主机的数目不大于 NAT 所拥有的合法公网 IP 地址的数目，采用此方法则可以保证每个内部地址都可以映射到一个公开的 IP 地址，否则允许同时连接到外部网络的内部主机的数目则会受到 NAT 公开 IP 地址数量的限制。

1.2.2 NAPT

NAPT（Network Address Port Translation）即网络端口地址转换，就是将多个内部地址映射为一个合法公网地址，但以不同的协议端口号与不同的内部地址相对应。也就是<**内部地址+内部端口**>与<**外部地址+外部端口**>之间的转换。NAPT 普遍用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。

NAPT 使得一组主机可以共享唯一的外部地址，当位于内部网络中的主机通过 NAT 设备向外部主机发起会话请求时，NAT 设备就会查询 NAT 表，看是否有相关会话记录，如果有相关记录，就会将内部 IP 地址及端口同时进行转换，再转发出去；如果没有相关记录，进行 IP 地址和端口转换的同时，还会在 NAT 表增加一条该会话的记录。外部主机接收到数据包后，用接受到的合法公网地址及端口作为目的 IP 地址及端口来响应，NAT 设备接收到外部回来的数据包，再根据 NAT 表中的记录把目的地址及端口转换成对应的内部 IP 地址及端口，转发给该内部主机。

以下给出了一个实例（如图 1-2），NAPT 的基本过程与 NAT 类似，所不同的是：NAPT 中内部端口与内部地址都进行了转换，而 NAT 中仅仅只对内部地址进行转换。

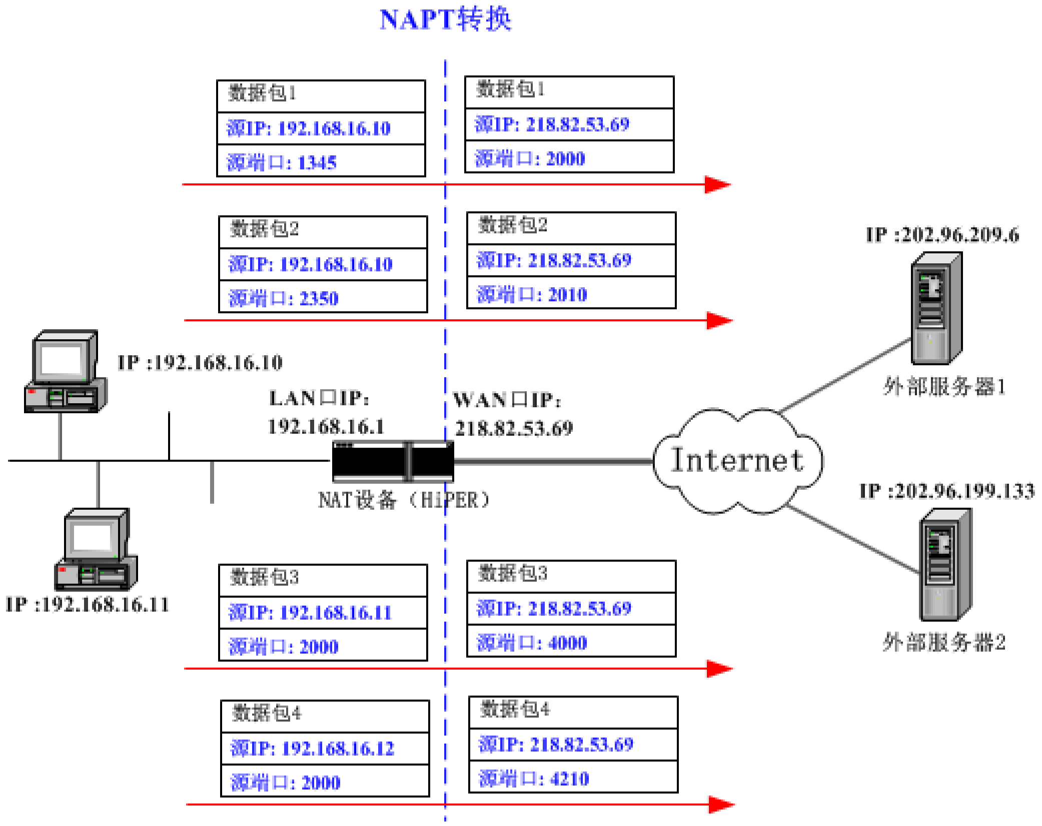

图 1-2 网络端口地址转换（NAPT）的基本过程

图 1-2 中，4 个带有内部地址的数据包到达 HiPER，其中数据包 1 和 2 来自同一个内部地址但有不同的源端口号，数据包 3 和 4 来自不同的内部地址但具有相同的源端口号。通过 NAPT，4 个数据包都被转换到同一个外部地址，但每个数据包都赋予了不同的源端口号，因此区分了这 4 个数据包。当回复数据包到达时，NAPT 就能根据回复数据包的目的地址和端口来区分该数据包应转发到的内部主机。

在 Internet 中使用 NAPT 时，所有不同的 TCP 和 UDP 信息流看起来好像来源于同一个 IP 地址。这种方式常用于拨号上网，通过从 ISP 处申请的一个 IP 地址，将多个连接通过 NAPT 接入 Internet。在实际使用中可以把 NAPT 和基本 NAT 结合起来，即将一组外部地址和端口转换结合起来。

第2章 HiPER 中 NAT 的实现

2.1 相关术语

在 HiPER 系列产品中，关于 NAT 的一些术语解释如下：

NAT 会话（NAT Session）：当内部网络中有主机向外发出连接请求时，HiPER 将会在 NAT 表中为该请求建立一条 NAT Session 的记录，从而将该主机内部的 IP 地址转化为合法的 IP 地址进行通信。这种由内到外、或者由外向内的连接就是一个 NAT Session。

NAT 规则（NAT Binding）：HiPER 支持使用不同的 NAT 类型及不同的公网 IP 地址配置多条 NAT 规则，NAT 规则决定会话的出口 IP 地址和端口。

EasyIP：NAT 类型之一，即 NAPT，可实现多个内部 IP 地址映射到同一个外部 IP 地址的不同端口上。

One2One：NAT 类型之一，即静态 NAT，可实现内部 IP 地址与外部 IP 地址建立一一对应的映射。

Passthrough：NAT 类型之一，可实现内部网络中的主机不做 NAT，直接路由出网。

内部 IP 地址（Internal IP）：内部网络中的主机所设置的 IP 地址，一般使用 RFC1918 规定的私有地址。

外部 IP 地址（Global IP）：内部 IP 地址通过 NAT（或 NAPT）后所映射的合法公网地址。

NAT 静态映射：通过定义服务端口，所有对 HiPER 该端口的服务请求将被重新定位给局域网中指定的服务器，从而外部网络中的计算机可通过 HiPER 访问指定的内部服务器。

虚拟服务器（DMZ 主机）：虚拟服务器（DMZ 主机）可以向 Internet 完全开放，以实现双向通信。

分配规则：用来控制线路流量所使用的规则，包括 NAT 会话和 IP 地址。

权重（weight）：只有“ EasyIP ”类型的 NAT 规则需要设置权重，使用各“ EasyIP ”NAT 规则的 NAT 会话（或 IP 地址）的数量比为它们的权重比。

2.2 NAT 功能介绍

2.2.1 概述

HiPER 系列产品支持 NAPT 和静态 NAT。通过选择不同的 NAT 类型及公网 IP 地址，可以配置多个 NAT 规则供用户使用，以满足用户的各种需要。用户可以通过配置 NAT 规则来指定某一范围内主机的上网线路，同时通过分配规则可实现对线路流量的控制，还可实现双线路带宽合并，以满足带宽要求高的应用需要。

HiPER 还支持一种特殊应用，即针对多媒体应用（比如 IP 语音和视频通讯会议）的实际需要，允许设置不进行地址转换、直接路由出网的内网主机。

同时，HiPER 还可通过配置 NAT 静态映射，实现外网主机对内部服务器的访问；通过配置虚拟服务器，实现将该 DMZ 主机完全暴露给 Internet，以进行双向通信。

2.2.2 NAT 地址空间

为了正确进行 NAT 操作，任何 NAT 设备都必须维护两个地址空间：一个是局域网主机在内部使用的私有 IP 地址，HiPER 中用“ 内部 IP 地址 ”表示；另一个是用于外部的公网 IP 地址，HiPER 中用“ 外部 IP 地址 ”表示。

2.2.3 三种 NAT 类型

HiPER 提供三种 NAT 类型：“ EasyIP ”、“ One2One ”及“ Passthrough ”。

EasyIP：即动态网络地址端口转换（动态 NAPT），多个内部 IP 地址映射到同一个外部 IP 地址。“ EasyIP ”NAT 可为每个内部连接动态分配一个与单一外部地址有关的端口，并维护这些内部连接到外部端口的映射，从而实现多个用户同时使用一个公网地址与外部 Internet 进行通信。

One2One：即静态地址转换（静态 NAT），内部 IP 地址与外部 IP 地址进行一对一的映射。“ One2One ”NAT 通常用来配置外网访问局域网的内部服务器：内部服务器依旧使用私有地址，对外提供为其分配的公网 IP 地址给外部网络用户访问。

Passthrough：对指定的 IP 地址不做 NAT，直接通过路由方式转发，它经常用于一些会受 NAT 影响制约的特别应用。比如，为保证 IP 语音和视频会议等应用的正常运行，可在内网中专门划分一个语音视频区，该区的主机均采用“ Passthrough ”方式。

我们将每个具体的 NAT 配置称为“ NAT 规则 ”，配置 NAT 规则时必须指定其出口 IP 地址及线路。当有多个合法的公网地址时，每种类型的 NAT 规则均可配置多个。实际应用中，常常需要混合使用不同类型的 NAT 规则。

2.2.4 主线路 NAT 规则和备份线路 NAT 规则

在 HiPER 中，我们将接在 WAN 口的线路称为主线路，将接在 WAN2/DMZ 口的线路称为备份线路。对于 HiPER 来说，无论是采取哪种上网方式：PPPoE 拨号方式、固定 IP 接入方式或者动态 IP 接入方式，如果要实现局域网用户共享一个或多个 IP 地址上网，都需要启用 NAT 功能，并设置对应的类型为“ EasyIP ”的 NAT 规则。

为了方便起见，我们定义了以下两个特殊的 NAT 规则：

主线路 NAT 规则：即外部 IP 地址为当前 WAN 口 IP 地址、类型为“ EasyIP ”的 NAT 规则；

备份线路 NAT 规则：即外部 IP 地址为当前 WAN2/DMZ 口 IP 地址、类型为“ EasyIP ”的 NAT 规则。

通常情况下，为了保证局域网用户正常上网，至少必须设置主线路（备份线路）NAT 规则。当然，如果某条上网线路分配了多个 IP 地址，还可以设置更多的不同类型的 NAT 规则。

2.2.5 根据源地址指定优先通道

在这里，通道是指上网使用的 NAT 规则，它决定了上网使用的 NAT 类型、外部 IP 地址（即出口 IP）及线路。

HiPER 允许用户预先为局域网中的某些主机指定优先通道，它是通过设置 NAT 规则的 “ 内部起始 IP 地址 ” 和 “ 内部结束 IP 地址 ” 来实现的，IP 地址属于两个地址范围内的主机将优先使用该 NAT 规则上网。对于已指定 NAT 规则的主机来说，当指定 NAT 规则可用时，它们只能使用该 NAT 规则上网；但是，当指定 NAT 规则失效时，HiPER 就把它们当作没有预先指定 NAT 规则的主机来处理。

2.2.6 根据线路带宽合理分配线路流量

HiPER 允许用户预先指定分配到两条线路的流量的比例，它是通过设置线路的 “ 权重 ” 来实现的。其中，线路的 “ 权重 ” 为绑定在该线路上的 NAT 规则的 “ 权重 ” 之和，需要注意的是，只有类型为 “ EasyIP ” 的 NAT 规则有 “ 权重 ”。

在实际应用中，当局域网中的主机均未指定 NAT 规则时，可根据两条线路的带宽比来设置各线路的 “ 权重 ”，从而实现按带宽分配流量。例如，主线路和备份线路的带宽分别为 6M、4M，若除了主线路 NAT 规则和备份线路 NAT 规则，还需配置一条绑定在主线路上的 “ EasyIP ”NAT 规则，则可将主线路 NAT 规则、新配 NAT 规则、备份线路 NAT 规则的 “ 权重 ” 分别设为 2、1、2。这样，主线路、备份线路的 “ 权重 ” 就分别为 3、2，分配到主线路、备份线路的流量比将接近 3:2。

而当局域网中的某些主机指定了上网线路时，若按照带宽比来设置线路的 “ 权重 ”，分配到两条线路的流量比可能会同带宽比相差较大。这时，可以根据实际情况适当调整‘ 权重 ”。

2.2.7 两种流量分配规则

“ 分配规则 ” 用来控制线路流量，它作用于局域网中没有预先指定 NAT 规则的计算机，HiPER 提供两种分配规则：“ NAT 会话 ” 和 “ IP 地址 ”，它们的实现机制如下所述。

1. IP 地址

使用 IP 地址作为分配规则时，HiPER 将根据 NAT 规则的 “ 权重 ”，把未指定 NAT 规则的主机的 IP 地址，按顺序依次分配到各 “ EasyIP ” NAT 规则。分配到各 “ EasyIP ” NAT 规则的 IP 地址的数量比为它们的 “ 权重 ” 比，来自同一 IP 地址的 NAT 会话使用同一个规则。

例如，若共有三条 “ EasyIP ” NAT 规则，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，第 1、2、3 台上网的主机将使用第一条规则，第 4、5 台主机将使用第二条规则，第 6 台主机将使用第三条规则，接着第 7、8、9 台主机将使用第一条规则，……，依此类推。注意，这里假设每台主机均只有一个 IP 地址。

2. NAT 会话

使用 NAT 会话作为分配规则时，HiPER 将根据 NAT 规则的“ 权重 ”，把未指定 NAT 规则的主机发起的 NAT 会话，按顺序依次分配到各“ EasyIP ”NAT 规则。分配到各“ EasyIP ” NAT 规则的 NAT 会话的数量比为它们的“ 权重 ”比，同一主机发起的 NAT 会话可使用多个 NAT 规则。

例如，若共有三条“ EasyIP ”NAT 规则，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，内网主机发起的第 1、2、3 个 NAT 会话将使用第一条规则，第 4、5 个 NAT 会话将使用第二条规则，第 6 个 NAT 会话将使用第三条规则，接着第 7、8、9 个 NAT 会话将使用第一条规则，……，依此类推。

一般情况下，建议“ 分配规则 ”选择为“ IP 地址 ”。当对带宽要求高，需要双线路带宽合并时，比如使用网络蚂蚁（NetAnts）、网际快车（FlashGet）、影像传送带（Net Transport）等多线程下载工具时（多线程下载指把一个下载文件分成若干份同时下载，下载后再把它们合并起来），则可选择“ NAT 会话 ”，从而能够充分利用双线路带宽，以提高下载速度。需要注意的是，即便选择了“ NAT 会话 ”，由于网站情况不同仍有可能造成带宽不能完全叠加的情况，同时还可能造成某些应用连接不畅。

2.2.8 NAT 静态映射

HiPER 系列产品集成了防火墙功能，在默认设置下，来自外部网络中的计算机无法通过防火墙的保护，因此无法通过 HiPER 访问内部网络中的某些服务器。而 HiPER 的 NAT 静态映射功能则可以解决这个问题，通过配置 NAT 静态映射，可将相应的外部 IP 地址、外部端口等映射到内部的服务器上，提供外部访问内部服务器（如 WWW、FTP 等服务）的功能。也就是说，用户可以通过由 NAT 静态映射定义的外部 IP 地址及外部端口来访问对应的内部服务器所提供的服务。

2.2.9 虚拟服务器（DMZ 主机）

某些情况下，需要将一台局域网计算机完全暴露给 Internet，以实现双向通信，这时候就需要将该计算机设置成虚拟服务器（DMZ 主机），被设置为虚拟服务器的计算机将失去 HiPER 的防火墙保护功能。当有外部用户访问为该 DMZ 主机分配的公网地址时，HiPER 会把数据包转发给指定的 DMZ 主机。

对于 HiPER 来说，当有多个公网 IP 地址时，可配置 1 个全局虚拟服务器，多个局部虚拟服务器。其中，局部虚拟服务器需指定其使用的 NAT 规则（类型为 EasyIP），该 NAT 规则的外部 IP 地址将分配给它，以提供给 Internet 上的主机访问时使用；全局虚拟服务器则无需指定。局部虚拟服务器比全局虚拟服务器的优先级高，只有在没有配置局部虚拟服务器时，才使用全局虚拟服务器。

另外，NAT 静态映射的优先级高于虚拟服务器。当 HiPER 收到一个来自外部网络的请求时，它将首先根据外部请求所请求服务的端口号，查看 NAT 静态映射列表，检查是否有匹配的 NAT 静态映射，如果有的话，就把请求消息发送到该 NAT 静态映射对应的局域网计算机上去。如果没有匹配的静态映射，才会检查是否有匹配的虚拟服务器。

2.2.10 NAT 规则的执行顺序

当局域网中有主机发起 NAT 访问时,会首先检查此计算机是否符合所有 NAT 规则中“ 内部起始 IP 地址 ”到“ 内部结束 IP 地址 ”所指定的范围。如果有匹配的规则，则使用该条规则上网。如果没有匹配的规则，则使用“ NAT 类型 ”为“ EasyIP ”的 NAT 规则上网；有多个“ EasyIP ”类型的 NAT 规则时，则根据“ 分配规则 ”为各条 NAT 规则分配流量，从而控制线路流量。

此外，如果系统中设置了静态路由（这里指主机路由或子网路由，不包括缺省路由，下同），那么，当局域网中有主机发起 NAT 访问时，将首先检查是否有匹配的静态路由，如果有，系统将通过该静态路由所指定的接口转发该数据包；如果没有匹配的静态路由，系统将按照上述 NAT 规则的执行顺序转发数据包。

2.3 NAT 转换表（NAT 会话表）

2.3.1 概述

HiPER 提供一个 NAT 转换表,用来记录地址端口转换的详细信息。由于 NAT 转换表中，每个表项都对应着局域网某个用户当前使用的某个 NAT 会话，它不仅记录了地址端口转换信息，也记录了与 NAT 会话相关的其他信息，因此，更多时候我们将之称为 NAT 会话表。可使用 **show ip nat translation** 等命令查看 NAT 会话表，具体参考章节 3.6.2。

该表中，每一条 NAT 会话包含内部 IP 地址、内部端口（即初始源端口）、外部端口（即经过 NAT 转换的源端口）、目的 IP 地址及端口、协议、发送/接收包的个数、产生该 NAT 会话的 NAT 规则（决定外部 IP 地址）、创建时间等信息。其中，内部 IP 地址、内部端口、外部端口、NAT 规则、协议、创建时间这几个参数就可以代表一个完整的地址端口转换记录；而且，由内部 IP 地址、内部端口以及协议可唯一确定一条地址端口转换记录。

NAT 会话表的最大总项数由系统预设（该值依赖于具体的产品型号，比如 3300NB 是 10000），不可修改。但是，可使用命令 **set ip nat maxsession** *maxsession* 统一配置局域网中每个用户能占用的最大会话数，详见章节 3.1.2。

2.3.2 NAT 转换表项（NAT 会话）的类型

如前所述，在 NAT 会话表中，每个 NAT 会话都包含它所使用的地址端口转换信息。根据生成机制的不同，我们可以将 NAT 会话分为两大类：

- 动态生成的 NAT 会话
- 使用 NAT 静态映射生成的 NAT 会话

以下两节将分别介绍它们。

2.3.3 动态生成的 NAT 会话

在这里，动态生成的 NAT 会话主要指由“ EasyIP ”或“ One2One ”类型的 NAT 规则动态生成的 NAT 会话，一般是局域网中某主机向外发出连接请求时，HiPER 使用与该主机匹配的 NAT 规则为该请求建立的 NAT 会话。另外，还包括 Internet 上的主机访问局域网内部提供的 DMZ 主机时动态生成的 NAT 会话；注意，当多个外部主机访问 DMZ 主机提供的某个服务时，系统将始终只显示最近那次访问产生的连接（NAT 会话）信息。

注意，可使用 **show ip nat translation** *BID* 命令查看当前使用某条指定 NAT 规则生成的全部 NAT 会话，*BID* 为该 NAT 规则的标识，参见章节 3.6.2。

一般在一台 PC 上打开一个门户网站主页，就会产生数十条乃至一百多个 NAT 会话。为了提高会话表项的利用率，HiPER 实行了会话超时机制，即当一个表项在一段时间内未使用后就认为该表项超时。系统针对不同的协议类型设置不同的超时时间，如 HTTP 是 10 分钟，DNS 1 分钟，普通 UDP 5 分钟，已建立的 TCP 会话是 12 个小时等。例如，某个 IP 地址为 192.168.16.139 的用户利用端口 1000 进行了一次对外 TCP 连接,系统通过 NAT 为它分配了相应的外部 IP 地址和外部端口，并在 NAT 会话表中增加一条相关记录，如果在 12 个小时内一直未使用这个 TCP 连接（即 NAT 会话），系统就认为该 NAT 会话超时。

一旦会话超时，虽然不会立即被删除，但是随时可能被新建立的 NAT 会话覆盖，这个过程称为重用（reuse）。出于算法和软件效率优化的需要，超时的会话表项一般只会被部分地重用；当 NAT 会话表满（即 NAT 会话表中的表项达到最大值）时，所有的超时会话就会一次性全部删除。

2.3.4 使用 NAT 静态映射生成的 NAT 会话

当配置了 NAT 静态映射之后,系统就会在 NAT 会话表中生成对应的端口地址转换记录，除非手工删除，该记录将一直存在。该记录包含如下信息：内部 IP 地址、内部端口、外部端口、NAT 规则（决定外部 IP 地址）、协议、创建时间。

当 Internet 上的某个主机访问内部某台主机对外提供的服务时，相关记录中就会增加当前这个连接（NAT 会话）的其余信息，比如目的 IP 地址、目的端口等。可使用 **show ip nat translation static** 命令查看所有的由 NAT 静态映射生成的端口地址转换记录（或 NAT 会话），参见章节 3.6.2、3.6.3。注意，当有多个主机访问该服务时，系统总是只显示最近那次访问产生的连接（NAT 会话）信息。

2.4 NAT ALG 功能

HiPER 的 NAT 模块不仅实现了一般的地址及端口转换功能，同时也支持 NAT ALG（Application Layer Gateways）功能，即应用层网关功能，使其可以支持各种特殊的应用协议。

这些特殊的应用协议的有效载荷中包含有 IP 地址和端口，然后又试图使用这些内嵌的 IP 地址和端口号建立连接，而 NAT ALG 功能则可对它们执行有效载荷的检测和变换，保证它们在 NAT 环境下的正常运行，无需用户做任何特殊配置。目前，HiPER 支持的特殊应用

协议包括：

- ICMP：全称为 Internet Control Message Protocol，即 Internet 控制消息协议；
- FTP：全称为 File Transfer Protocol，即文件传输协议；
- GRE：全称为 Generic Routing Encapsulation，即基本路由封装协议。
- PPTP：全称为 Point-to-Point Tunneling Protocol，即点对点隧道协议；通过 PPTP 隧道传输数据时，使用 GRE 协议封装 PPP 数据包。
- ESP：全称为 Encapsulating Security Payload，即封装安全负荷，属于 IPSec 的一种协议。

第3章 NAT 配置

3.1 NAT 全局配置

NAT 全局配置包括以下几个方面的内容：

- 启用/禁用 NAT 功能
- 设置最大 NAT 会话数
- 设置分配规则

3.1.1 启用/禁用 NAT 功能

缺省情况下，系统是禁用 NAT 功能的。因此，首先需要启用 NAT 功能，局域网计算机才能实现共享上网。

配置命令如表 3-1 所示。

操作	命令
启用 NAT 功能	**set ip nat routing enabled**
禁用 NAT 功能	**set ip nat routing disabled**
备注：缺省情况下，为禁用 NAT 功能。	

表 3-1 启用/禁用 NAT 功能

提示：在 WEB UI 中配置时，当 ***WEB 管理界面—>基本配置—>快速向导***或 ***WEB 管理界面—>基本配置—>ISP 配置***界面中配置完上网连接线路后，HiPER 会自动打开 NAT 功能。除非特别需要，请不要关闭此功能，否则 HiPER 将失去共享上网功能。

3.1.2 设置最大 session 数

“ 最大 session 数 ” 是指局域网中单个用户的 NAT 最大并发连接数，它是 HiPER 的防火墙防止 DDOS 攻击的参数之一。通过设置 “ 最大 session 数 ” 可以避免因局域网某台主机申请过多的 NAT 会话，从而导致其他局域网主机没有 NAT 会话资源的现象。缺省情况下，该参数的值为 1200，一般无需修改。

当某些局域网应用（比如网络游戏）发生连接速度变慢的情况时，可以适当提高 “ 最大 Session 数 ”。注意，“ 最大 Session 数 ”设置过高可能会导致 HiPER 减弱甚至丧失防止 DDoS 攻击的功能，建议该值在 800～1200 之间。

配置命令如表 3-2 所示。

操作	命令
设置最大 session 数	**set ip nat maxsession** *maxsession*
备注：“ **maxsession** ” 缺省值为 1200。	

表 3-2 设置最大 session 数

3.1.3 设置分配规则

“ 分配规则 ”用来控制线路流量，它作用于局域网中没有预先指定 NAT 规则的计算机，HiPER 提供两种分配规则：“ NAT 会话 ” 和 “ IP 地址 ”，具体涵义及用法请参考章节 2.2.7。

配置命令如表 3-3 所示。

操作	命令
设置分配规则为 IP 地址	**set ip nat hostSpanIf no**
设置分配规则为 NAT 会话	**set ip nat hostSpanIf yes**
备注：缺省情况下，使用 IP 地址作为分配规则。	

表 3-3 设置分配规则

3.2 NAT 规则配置

如章节 2.2.3 所述，HiPER 提供三种类型的 NAT 规则：EasyIP、One2One 以及 Passthrough。由于这三种类型的 NAT 规则的配置各自不同，因此，以下各节将分别介绍它们的配置方法及注意事项。

3.2.1 NAT 规则配置——EasyIP 类型

EasyIP 类型的 NAT 规则配置主要包括以下几个方面的内容：

- 新建一条 NAT 规则
- 设置 NAT 规则的类型为 EasyIP
- 设置外部 IP 地址
- 设置内部起始 IP 地址和内部结束 IP 地址
- 设置权重
- 设置绑定线路（端口）
- 启用/禁用一条 NAT 规则
- 删除一条 NAT 规则

此外，局部 DMZ 主机也是在 EasyIP 类型的规则中配置，具体请参考章节 3.4.2。

3.2.1.1 新建一条 NAT 规则

首先需要创建一条 NAT 规则，并为该 NAT 规则自定义一个名称。

配置命令如表 3-4 所示。

操作	命令
新建一条 NAT 规则	**new ip nat binding/***binding-name*
备注：“ *binding-name* ” 为用户自定义的 NAT 规则的名称。	

表 3-4 新建一条 NAT 规则——EasyIP

3.2.1.2 设置 NAT 规则的类型为 EasyIP

HiPER 支持 3 种类型的 NAT 规则，这里需将 NAT 规则的类型设置为 EasyIP。由于缺省情况下，NAT 规则类型为 EasyIP，因此，无需修改缺省配置。

配置命令如表 3-5 所示。

操作	命令
设置 NAT 规则的类型为 EasyIP	**set ip nat binding/***binding-name* **natmethod easyip**
备注：缺省情况下，NAT 规则类型为 EasyIP。	

表 3-5 设置 NAT 规则的类型为 EasyIP

3.2.1.3 设置外部 IP 地址

外部 IP 地址是指：该 NAT 规则中，内部 IP 地址所映射的公网 IP 地址。设置主线路（备份线路）NAT 规则时，使用缺省配置 0.0.0.0，表示默认使用广域网端口当前的 IP 地址，不能修改；同时，配置其余本类型规则时，只能使用由 ISP 分配的 WAN 口（或 WAN2 口）以外的 IP 地址作为映射地址，不能使用 0.0.0.0。

主线路 NAT 规则及备份线路 NAT 规则的涵义请参考章节 2.2.4。

配置命令如表 3-6 所示。

操作	命令
设置 NAT 规则对应的外部 IP 地址	**set ip nat binding/***binding-name* **globalip** *globalip*
备注：“ **globalip** ” 缺省值为 0.0.0.0。	

表 3-6 设置 NAT 规则对应的外部 IP 地址——EasyIP

3.2.1.4 设置内部起始 IP 地址和内部结束 IP 地址

内部结束 IP 地址必须大于内部起始 IP 地址，通过这两个参数可定义一段连续的地址范围，该范围内的局域网计算机将优先使用该 NAT 规则上网。

配置命令如表 3-7 所示。

操作	命令
设置内部起始 IP 地址	**set ip nat binding/***binding-name* **internalipfrom** *from-ip*
设置内部结束 IP 地址	**set ip nat binding/***binding-name* **internalipto** *to-ip*
备注：缺省情况下，“ **internalipfrom** ” 和 “ **internalipto** ” 的值都为 0.0.0.0。	

表 3-7 设置内部起始 IP 地址和内部结束 IP 地址——EasyIP

3.2.1.5 设置权重

如章节 2.2.6 及 2.2.7 所述，通过设置各条 EasyIP 类型的 NAT 规则的 “ 权重 ”，可以实现根据线路带宽合理分配线路流量。

配置命令如表 3-8 所示。

操作	命令
设置 NAT 规则的权重	**set ip nat binding/***binding-name* **weight** *weight*
备注：“ **weight** ” 缺省值为 1。	

表 3-8 设置 NAT 规则的权重——EasyIP

3.2.1.6 设置绑定线路（端口）

另外，还需指定 NAT 规则的绑定线路（端口），通过该 NAT 规则产生的 NAT 会话将使用指定的绑定线路。

若绑定的线路使用固定 IP 接入方式或动态 IP 接入方式，该参数（profile）的值为相关物理端口的端口名，LAN 口、WAN 口、WAN2/DMZ 口对应的端口名分别为：eth1、eth2、eth3；若绑定的线路 PPPoE 拨号上网线路或 PPTP/L2TP VPN 隧道连接，该参数的值为相关连接的连接实例名。

配置命令如表 3-9 所示。

操作	命令
设置 NAT 规则的绑定端口	**set ip nat binding/***binding-name* **profile** *interface*
备注：“ **profile** ” 的缺省值为空。	

表 3-9 设置 NAT 规则的绑定线路（端口）——EasyIP

3.2.1.7 启用/禁用一条 NAT 规则

允许设置各条 NAT 规则的使能状态：启用或禁用。如果你暂时不需要使用某条 NAT 规则，只需禁用它即可，此时该 NAT 规则仅在配置文件中可见，但不再有效；当需要恢复使用该 NAT 规则时，只需启用它即可。

配置命令如表 3-10 所示。

操作	命令
启用一条 NAT 规则	**set ip nat binding/***binding-name* **enabled yes**
禁用一条 NAT 规则	**set ip nat binding/***binding-name* **enabled no**
备注：缺省情况下，为启用 NAT 规则。	

表 3-10 启用/禁用一条 NAT 规则——EasyIP

3.2.1.8 删除一条 NAT 规则

如有需要，可删除已配置的 NAT 规则，一次只能删除一条。

配置命令如表 3-11 所示。

操作	命令
删除一条 NAT 规则	**delete ip nat binding/***binding-name*
备注：删除某条 NAT 规则时，输入的“*binding-name*”必须与新建该 NAT 规则时输入的名字全字匹配。	

表 3-11 删除一条 NAT 规则——EasyIP

3.2.2 NAT 规则配置——One2One 类型

One2One 类型的 NAT 规则配置主要包括以下几个方面的内容：

- 新建一条 NAT 规则
- 设置 NAT 规则的类型为 One2One
- 设置外部起始 IP 地址
- 设置内部起始 IP 地址和内部结束 IP 地址
- 设置绑定线路
- 启用/禁用一条 NAT 规则
- 删除一条 NAT 规则

3.2.2.1 新建一条 NAT 规则

首先需要创建一条 NAT 规则，并为该 NAT 规则自定义一个名称。

配置命令如表 3-12 所示。

操作	命令
新建一条 NAT 规则	**new ip nat binding/***binding-name*
备注：“ *binding-name* ” 为用户自定义的 NAT 规则的名称。	

表 3-12 新建一条 NAT 规则——One2One

3.2.2.2 设置 NAT 规则的类型为 One2One

HiPER 支持 3 种类型的 NAT 规则，这里需将 NAT 规则的类型设置为 One2One。由于缺省情况下，NAT 规则类型为 EasyIP，因此，必须修改缺省配置。

配置命令如表 3-13 所示。

操作	命令
设置 NAT 规则的类型为 One2One	**set ip nat binding/***binding-name* **natmethod one2one**
备注：缺省情况下，NAT 规则类型为 EasyIP。	

表 3-13 设置 NAT 规则的类型为 One2One

3.2.2.3 设置外部起始 IP 地址

外部起始 IP 地址：该 NAT 规则中，内部起始 IP 地址所映射的外部起始 IP 地址。外部起始 IP 地址必须设置，实际映射的外部地址是从设置值开始向上依次增加。

例如，如果“ 内部起始 IP 地址 ”设为 192.168.16.6，“ 内部结束 IP 地址 ”设为 192.168.16.8，“ 外部起始 IP 地址 ” 设为 200.200.200.116，则 192.168.16.6、192.168.16.7、192.168.16.8 依次映射成 200.200.200.116、200.200.200.117、200.200.200.118。

配置命令如表 3-14 所示。

操作	命令
设置 NAT 规则对应的外部起始 IP 地址	**set ip nat binding/***binding-name* **globalip** *globalip*
备注：“ **globalip** ” 缺省值为 0.0.0.0。	

表 3-14 设置 NAT 规则对应的外部起始 IP 地址——One2One

3.2.2.4 设置内部起始 IP 地址和内部结束 IP 地址

内部结束 IP 地址必须大于内部起始 IP 地址，通过这两个参数可定义一段连续的地址范围，该范围内的局域网计算机将使用 “ One2One ” 类型的 NAT 规则访问 Internet。事实上，该范围内的每个内部 IP 地址都将分别映射成一个外部地址，详见章节 3.2.2.3。

配置命令如表 3-15 所示。

操作	命令
设置内部起始 IP 地址	**set ip nat binding/***binding-name* **internalipfrom** *from-ip*
设置内部结束 IP 地址	**set ip nat binding/***binding-name* **internalipto** *to-ip*
备注：缺省情况下，“ **internalipfrom** ”和“ **internalipto** ”的值都为 0.0.0.0。	

表 3-15 设置内部起始 IP 地址和内部结束 IP 地址——One2One

3.2.2.5 设置绑定线路（端口）

另外，还需指定 NAT 规则的绑定线路（端口），通过该 NAT 规则产生的 NAT 会话将使用指定的绑定线路。

若绑定的线路使用固定 IP 接入方式或动态 IP 接入方式，该参数（profile）的值为相关物理端口的端口名，LAN 口、WAN 口、WAN2/DMZ 口对应的端口名分别为：eth1、eth2、eth3；若绑定的线路 PPPoE 拨号上网线路或 PPTP/L2TP VPN 隧道连接，该参数的值为相关连接的连接实例名。

配置命令如表 3-16 所示。

操作	命令
设置 NAT 规则的绑定线路	**set ip nat binding/***binding-name* **profile** *interface*
备注：“ **profile** ”的缺省值为空。	

表 3-16 设置 NAT 规则的绑定线路（端口）——One2One

3.2.2.6 启用/禁用一条 NAT 规则

允许设置各条 NAT 规则的使能状态：启用或禁用。如果你暂时不需要使用某条 NAT 规则，只需禁用它即可，此时该 NAT 规则仅在配置文件中可见，但不再有效；当需要恢复使用该 NAT 规则时，只需启用它即可。

配置命令如表 3-17 所示。

操作	命令
启用一条 NAT 规则	**set ip nat binding/***binding-name* **enabled yes**
禁用一条 NAT 规则	**set ip nat binding/***binding-name* **enabled no**
备注：缺省情况下，为启用 NAT 规则。	

表 3-17 启用/禁用一条 NAT 规则——One2One

3.2.2.7 删除一条 NAT 规则

如有需要，可删除已配置的 NAT 规则，一次只能删除一条。

配置命令如表 3-18 所示。

操作	命令
删除一条 NAT 规则	**delete ip nat binding/***binding-name*
备注：删除某条 NAT 规则时，输入的“ *binding-name* ”必须与新建该 NAT 规则时输入的名字全字匹配。	

表 3-18 删除一条 NAT 规则——One2One

3.2.3 NAT 规则配置——Passthrough 类型

Passthrough 类型的 NAT 规则配置主要包括以下几个方面的内容：

- 新建一条 NAT 规则
- 设置 NAT 规则的类型为 Passthrough
- 设置内部起始 IP 地址和内部结束 IP 地址
- 设置绑定线路
- 启用/禁用一条 NAT 规则
- 删除一条 NAT 规则

3.2.3.1 新建一条 NAT 规则

首先需要创建一条 NAT 规则，并为该 NAT 规则自定义一个名称。

配置命令如表 3-19 所示。

操作	命令
新建一条 NAT 规则	**new ip nat binding/***binding-name*
备注：“ *binding-name* ”为用户自定义的 NAT 规则的名称。	

表 3-19 新建一条 NAT 规则——Passthrough

3.2.3.2 设置 NAT 规则的类型为 Passthrough

HiPER 支持 3 种类型的 NAT 规则，这里需将 NAT 规则的类型设置为 Passthrough。由于缺省情况下，NAT 规则类型为 EasyIP，因此，必须修改缺省配置。

配置命令如表 3-20 所示。

操作	命令

设置 NAT 规则的类型为 Passthrough	**set ip nat binding/***binding-name* **natmethod passthrough**
备注：缺省情况下，NAT 规则类型为 EasyIP。	

表 3-20 设置 NAT 规则的类型为 Passthrough

3.2.3.3 设置内部起始 IP 地址和内部结束 IP 地址

内部起始IP地址和内部结束IP地址，就是指局域网中使用该NAT规则、通过Passthrough方式上网的计算机的起始和结束 IP 地址，内部结束 IP 地址必须大于内部起始 IP 地址，这两个地址范围之内的 IP 地址不能与其他规则的外部 IP 地址重叠。

配置命令如表 3-21 所示。

操作	命令
设置内部起始 IP 地址	**set ip nat binding/***binding-name* **internalipfrom** *from-ip*
设置内部结束 IP 地址	**set ip nat binding/***binding-name* **internalipto** *to-ip*
备注：缺省情况下，“ **internalipfrom** ”和“ **internalipto** ”值都为 0.0.0.0。	

表 3-21 设置内部起始 IP 地址和内部结束 IP 地址——Passthrough

3.2.3.4 设置绑定线路（端口）

另外，还需指定 NAT 规则的绑定线路（端口），通过该 NAT 规则产生的 NAT 会话将使用指定的绑定线路。

若绑定的线路使用固定 IP 接入方式或动态 IP 接入方式，该参数（profile）的值为相关物理端口的端口名，LAN 口、WAN 口、WAN2/DMZ 口对应的端口名分别为：eth1、eth2、eth3；若绑定的线路 PPPoE 拨号上网线路或 PPTP/L2TP VPN 隧道连接，该参数的值为相关连接的连接实例名。

配置命令如表 3-22 所示。

操作	命令
设置 NAT 规则的绑定线路	**set ip nat binding/***binding-name* **profile** *interface*
备注：“ **profile** ”的缺省值为空。	

表 3-22 设置 NAT 规则的绑定线路（端口）——Passthrough

3.2.3.5 启用/禁用一条 NAT 规则

允许设置各条 NAT 规则的使能状态：启用或禁用。如果你暂时不需要使用某条 NAT 规则，只需禁用它即可，此时该 NAT 规则仅在配置文件中可见，但不再有效；当需要恢复使用该 NAT 规则时，只需启用它即可。

配置命令如表 3-23 所示。

操作	命令
启用一条 NAT 规则	**set ip nat binding/***binding-name* **enabled yes**
禁用一条 NAT 规则	**set ip nat binding/***binding-name* **enabled no**
备注：缺省情况下，为启用 NAT 规则。	

表 3-23 启用/禁用一条 NAT 规则——Passthrough

3.2.3.6 删除一条 NAT 规则

如有需要，可删除已配置的 NAT 规则，一次只能删除一条。

配置命令如表 3-24 所示。

操作	命令
删除一条 NAT 规则	**delete ip nat binding/***binding-name*
备注：删除某条 NAT 规则时，输入的“ *binding-name* ”必须与新建该 NAT 规则时输入的名字全字匹配。	

表 3-24 删除一条 NAT 规则——Passthrough

3.3 NAT 静态映射配置

NAT 静态映射配置主要包括以下几个方面的内容：

- 新建一条 NAT 静态映射
- 设置协议类型
- 设置内部 IP 地址
- 设置内部起始端口
- 设置外部起始端口
- 设置端口浮动范围
- 设置绑定的 NAT 规则
- 启用/禁用一条 NAT 静态映射
- 删除一条 NAT 静态映射

3.3.1 新建一条 NAT 静态映射

首先需要创建一条 NAT 规则，并为该 NAT 规则自定义一个名称。

配置命令如表 3-25 所示。

操作	命令

新建一条 NAT 规则	**new ip nat static/***staticmap-name*
备注：“ *mapping-name* ” 为用户自定义的 NAT 静态映射的名称。	

表 3-25 新建一条 NAT 静态映射

3.3.2 设置协议类型

首先，需要设置 NAT 静态映射提供的服务所使用的协议类型。一般情况下，协议类型选择为 TCP，UDP 或 GRE 协议。其中，GRE 协议在 PPTP 隧道时使用。

配置命令如表 3-26 所示。

操作	命令
设置 NAT 静态映射的协议类型	**set ip nat static/***staticmap-name* **protocol** {**tcp**｜**udp**｜**gre**}
备注：“ **protocol** ” 缺省值为 TCP。	

表 3-26 设置 NAT 静态映射的协议类型

3.3.3 设置内部 IP 地址

内部 IP 地址是指局域网中作为服务器的计算机的 IP 地址。

配置命令如表 3-27 所示。

操作	命令
设置 NAT 静态映射的内部 IP 地址	**set ip nat static/***staticmap-name* **localaddress** *localaddress*
备注：“ **localaddress** ” 缺省值为 0.0.0.0。	

表 3-27 设置 NAT 静态映射的内部 IP 地址

3.3.4 设置内部起始端口

局域网服务器提供的服务的起始端口。

配置命令如表 3-28 所示。

操作	命令
设置 NAT 静态映射的内部起始端口	**set ip nat static/***staticmap-name* **localport** *localport*
备注：“ **localport** ” 缺省值为 0。	

表 3-28 设置 NAT 静态映射的内部起始端口

3.3.5 设置外部起始端口

内部起始端口通过 NAT 所映射的外部起始端口，即 HiPER 提供给 Internet 的起始服务端口。

配置命令如表 3-29 所示。

操作	命令
设置 NAT 静态映射的外部起始端口	**set ip nat static/***staticmap-name* **dstport** *dstport*
备注：“ **dstport** ” 缺省值为 0。	

表 3-29 设置 NAT 静态映射的内部起始端口

3.3.6 设置端口浮动范围

某些时候，需要映射的不止一个端口，这时就必须设置端口浮动范围，端口浮动范围的值为端口数量的值减去 1。例如，若内部起始端口为 21，外部起始端口为 21，那么端口浮动范围的值为 20 时，则表示共有 21 个映射端口，内部端口范围为：21~41，同时外部端口与之一一对应，范围相应为：21～41。

配置命令如表 3-30 所示。

操作	命令
设置 NAT 静态映射的端口浮动范围	**set ip nat static/***staticmap-name* **dstrange** *dstrange*
备注：“ **dstrange** ” 缺省值为 0。	

表 3-30 设置 NAT 静态映射的端口浮动范围

3.3.7 设置绑定的 NAT 规则

另外，还需指定 NAT 静态映射所绑定的 NAT 规则。设置绑定的 NAT 规则时，参数 “ **binding** ” 的值为欲绑定的 NAT 规则的名称。

注意，只允许将 NAT 静态映射绑定到 “ EasyIP ” 类型的 NAT 规则上，该 NAT 规则的外部 IP 地址即为 NAT 静态映射的外部 IP 地址。

配置命令如表 3-31 所示。

操作	命令
设置 NAT 静态映射绑定的 NAT 规则	**set ip nat static/***staticmap-name* **binding** *binding-name*
备注：“ **binding** ” 的缺省值为空，	

表 3-31 设置 NAT 静态映射所绑定的 NAT 规则

3.3.8 启用/禁用一条 NAT 静态映射

允许设置各条 NAT 静态映射的使能状态：启用或禁用。如果你暂时不需要使用某条 NAT 静态映射，只需禁用它即可，此时该 NAT 静态映射仅在配置文件中可见，但不再有效；当需要恢复使用该 NAT 静态映射时，只需启用它即可。

配置命令如表 3-32 所示。

操作	命令
启用一条 NAT 静态映射	**set ip nat static/***staticmap-name* **enabled yes**
禁用一条 NAT 静态映射	**set ip nat static/***staticmap-name* **enabled no**
备注：缺省情况下，为启用 NAT 静态映射。	

表 3-32 启用/禁用一条 NAT 静态映射

3.3.9 删除一条 NAT 静态映射

如有需要，可删除已配置的 NAT 静态映射，一次只能删除一条。

配置命令如表 3-33 所示。

操作	命令
删除一条 NAT 静态映射	**delete ip nat static/***staticmap-name*
备注：删除 NAT 静态映射时，输入的“ *mapping-name* ”必须与新建该 NAT 映射时输入的名字全字匹配。	

表 3-33 删除一条 NAT 静态映射

3.4 DMZ 主机的配置

如章节 2.2.9 所述，HiPER 中可设置一个全局 DMZ 主机，多个局部 DMZ 主机。注意，被设置为 DMZ 主机的局域网计算机将失去 HiPER 的防火墙保护功能。

3.4.1 设置全局 DMZ 主机

HiPER 中，允许设置一个全局 DMZ 主机，全局 DMZ 主机作用于系统设置的所有类型为“ EasyIP ”的 NAT 规则。

配置命令如表 3-34 所示。

操作	命令
设置全局 DMZ 主机	**set ip nat defsvr** *dmz-ip*
备注：“ **defsvr** ” 缺省值为 0.0.0.0。	

表 3-34 设置全局 DMZ 主机

提示：如果配置了全局 DMZ 主机，HiPER 就允许从外网对 WAN 口和 WAN2/DMZ 口执行 ping 命令。

3.4.2 设置局部 DMZ 主机

HiPER 中，允许为每个类型为“ EasyIP ”的 NAT 规则分别设置局部 DMZ 主机，局部 DMZ 主机仅作用于当前指定的 NAT 规则。局部 DMZ 主机的优先级高于全局 DMZ 主机的优先级。

配置命令如表 3-35 所示。

操作	命令
设置局部 DMZ 主机	**set ip nat binding/***binding-name* **defaultserver** *dmz-ip*
备注：“ *binding-name* ” 为欲设置局部 DMZ 主机的 NAT 规则的名称； “ **defaultserver** ” 缺省值为 0.0.0.0。	

表 3-35 设置局部 DMZ 主机

提示：如果在主线路 NAT 规则中设置了局部 DMZ 主机，HiPER 就允许从外网对 WAN 口执行 ping 命令；同样地，只要在备份线路 NAT 规则中设置了局部 DMZ 主机，HiPER 就允许从外网对 WAN2/DMZ 口执行 ping 命令。

3.5 NAT 配置的注意事项

HiPER 中，要保证 NAT 正常工作，还需注意以下事项，并进行相关配置。

1. 必须启用快速转发功能

配置命令为：

```
！启用快速转发功能
set system l3Switch enabled
```

2. 如果 WAN 口（或 WAN2/DMZ 口）为多地址接入，必须启用 NAT 类型的 ARP 代理功能

1） WAN 口多地址接入时，配置命令为：

```
！在 WAN 口启用 NAT 类型的 ARP 代理功能
set interface ethernet/2 ip arpproxy nat
```

2) WAN2/DMZ 口多地址接入时，配置命令为：

！在 WAN2/DMZ 口启用 NAT 类型的 ARP 代理功能

```
set interface ethernet/3 ip arpproxy nat
```

3. **如果 WAN 口（或 WAN2/DMZ 口）为多地址接入，局域网主机要访问 ISP 分配的当前广域网端口 IP 地址之外的公网 IP 地址时，需配置相关的静态路由。**

主要应用：

使用 EasyIP 类型的 NAT 规则的局域网主机要通过公网地址访问“ **One2One** ”类型的 NAT 规则所指定的内部主机时，需设置相关的静态路由。

一般情况下，相关的静态路由为主机路由，其目的地址为需要访问的公网地址，掩码为 255.255.255.255，网关为对应的广域网端口当前使用的 IP 地址。因此，如果需要访问多个 IP 地址，则需要设置多条主机路由。

当然，如果某些待访问的公网地址可以划分在同一个子网（该子网地址数更少，不能包括当前广域网端口 IP 地址）中，也可以通过为它们设置一条子网路由来实现：其目的地址为新的子网的网络号，掩码为新的子网掩码，网关仍为对应的广域网端口当前使用的 IP 地址。

一般情况下，为避免无谓的错误，采用设置主机路由的方式即可。

1) 设置相关的主机路由时，配置命令为：

！新建一条主机路由，自定义路由名

new ip route static/*route-name*

！设置主机路由的目的 IP 地址(为内部主机要访问的公网 IP 地址)

set ip route static/route-name dest *dest-ip*

！设置主机路由的子网掩码

set ip route static/route-name netmask 255.255.255.255

！设置主机路由的网关地址（为对应的广域网端口当前使用的 IP 地址）

set ip route static/route-name gateway *gateway-ip*

2) 设置相关的子网路由时，配置命令类似，只需将目的 IP 地址设为新的子网的网络号，将子网掩码设为新的子网掩码即可，这里不再详述。

3.6 NAT 的显示和诊断

3.6.1 查看 NAT 摘要信息

在 HiPER 中，可以查看 NAT 摘要信息，包括已设置的 NAT 规则的配置信息、以及系统全部 NAT 会话的统计信息等。

配置命令如表 3-36 所示。

操作	命令

查看 NAT 摘要信息	**show ip nat summary**

表 3-36 查看 NAT 摘要信息

以下提供了一个使用命令“ **show ip nat summary** ”查看 NAT 摘要信息的实例（如图 3-1），并结合该例对相关参数进行描述和说明。

```
hiper% show ip nat summary
Nat bindings list

BID   LIPFrom     LIPTo        GlobalIP     M    Name       IF    Wgt  Ref
A     0.0.0.0    0.0.0.0    222.64.24.222   E   PEBIND    ptp0    1     0

nat binding total item 60, inuse 1

nat hostSpan 1, udpSpan 0, natEnable 1

Table total item inuse count 95
Table total item count 140, max 10000

Maximum depth of forward hash is 5
Maximum depth of backward hash is 2

Table full fail count 2, last 5164 seconds ago

Forward total 13846
Forward map fail 5

Backward total 2012
Backward map fail 6141
```

图 3-1 查看 NAT 摘要信息

图 3- 1 中，NAT 摘要信息中各信息涵义如下所述。

1. Nat bindings list：NAT 规则列表。该表中各参数涵义如下：

- BID：NAT 规则的标识，按照配置的顺序，从上往下依次为 A、B、C 、……、。
- LIPFrom：该 NAT 规则的内部起始 IP 地址。
- LIPTo：该 NAT 规则内部结束 IP 地址。
- GlobalIP：该 NAT 规则的外部 IP 地址。
- M：该 NAT 规则的类型。其中，E-类型为 EasyIP，O-类型为 One2One，P-类型为 Passthrogh。
- Name：该 NAT 规则的名称。
- IF：该 NAT 规则绑定的端口。
- Wgt：该 NAT 规则的权重值，尽对“ EasyIP ”类型的 NAT 规则有意义。
- Ref：该 NAT 规则的新建次数。

2. nat binding total item 60, inuse 1：可设置的 NAT 规则的最大数目为 60，当前设置了 1 条 NAT 规则。

3. nat hostSpan 1，udpSpan 0，natEnable 1：nat hostSpan 指设置的分配规则，1 代表分配规则为 NAT 会话，0 代表分配规则为 IP 地址；udpSpan 指 udp 类型的 NAT 会话是否做负载均衡，1 代表做负载均衡，0 代表不做负载均衡；natEnable 指是否启用

NAT 功能，1 代表启用，0 代表禁用。

4. Table total item inuse count 95：NAT 会话表中当前正在使用（未超时）的 NAT 会话数为 95。
   Table total item count 140，max 10000：NAT 会话表中当前存在的全部（包括超时）NAT 会话数为 140，NAT 会话表所能提供的最大总项数为 1000。
5. Maximum depth of forward hash is 5：会话前向 HASH 查找深度。
   Maximum depth of backward hash is 2：会话方向 HASH 查找深度。
6. table full fail count 2, last 5164 seconds ago：发生 NAT 会话表满（即 NAT 会话表中的表项达到最大值）的次数为 2 次，上次发生时间为 5164 秒之前。
7. forward total 13846：NAT 翻译成功的总次数。
   forward map fail 5：NAT 翻译失败的次数，一般由局域网某用户使用 NAT 会话数量超限引起。
8. backward map 2012：NAT 反向翻译成功的总次数。
   backward map fail 6141：NAT 反向翻译失败的次数，一般由非正常外部访问引起。

3.6.2 查看 NAT 会话表

在 HiPER 中，可以查看局域网内部当前进行的全部 NAT 会话信息，还可查看由 NAT 静态映射产生的 NAT 会话信息，也可查看由某条 NAT 规则产生的所有 NAT 会话信息，参见章节 2.3。

配置命令如表 3-37 所示。

操作	命令
查看全部 NAT 会话信息	**show ip nat translation**
查看由 NAT 静态映射产生的 NAT 会话信息	**show ip nat translation static**
查看使用某条 NAT 规则产生的 NAT 会话信息	**show ip nat translation** *BID*
备注：“ BID ” 为 NAT 规则实例的标识，具体涵义参考章节 3.6.1。	

表 3-37 查看 NAT 会话表

以下提供了一个使用命令“ **show ip nat translation** ”查看全部 NAT 会话信息的实例（如图 3-2），并结合该例对相关参数进行描述和说明。

```
hiper% show ip nat translation
NO      SrcIP      SrcPORT          DestIP  DestPORT  P  OutPkt   InPkt  GPORT  BID  AGE
1   200.200.200.50    6006   219.133.38.66        qq  U      66      64   3040    A   12
2   200.200.200.50    3389    61.130.74.22      6000  T    1849    1195   3389    A  760
3   200.200.200.54     ntp    208.184.49.9       ntp  U      16      16   3525    B   43
4   200.200.200.87    1642  218.95.162.149      5100  T       2       0   5510    B   52
5   200.200.200.87    1533   61.152.199.13     12260  T    1573    1040   3125    B    2
6   218.82.48.103     1130    202.96.209.5       dns  U       1       1   5507    B   58
7   218.82.48.103      ntp   192.43.244.18       ntp  U      16      16   3036    A  290
8   218.82.48.103     l2tp         0.0.0.0         0  U       0       0   l2tp    A 4798
9   200.200.200.139   1804     207.46.0.32       msn  T     275     209   3166    A   17

   ......  ......

91 200.200.200.25  telnt         0.0.0.0         0  T       0       0 telnt    A 4798

Totally 91 items
```

图 3-2 查看 NAT 会话信息

图 3- 2 中，NAT 会话信息中各个参数涵义如下：

- NO：序号。
- SrcIP：NAT 会话的源 IP 地址，即局域网内对应主机的 IP 地址。
- SrcPORT：NAT 会话的源端口，即局域网内对应主机使用的端口。若为周知端口，显示其服务名（如 TCP 协议的 80 端口显示为 http）；否则直接显示端口号。
- DestIP：NAT 会话的目的 IP 地址，即 Internet 上的对端设备的 IP 地址。
- DestPORT：NAT 会话的目的端口，即 Internet 上的对端设备使用的服务端口。若为周知端口，显示其服务名（如 TCP 协议的 80 端口显示为 http）；否则直接显示端口号。
- P：NAT 会话的协议类型。其中，G-GRE 协议，T-TCP 协议，U-UDP 协议。
- OutPkt：局域网主机通过该 NAT 会话发送的数据包数量的统计。
- InPkt：局域网主机通过该 NAT 会话接收的数据包数量的统计。
- GPORT：该 NAT 会话所映射的外部端口。
- BID：NAT 规则实例的标识。按照配置顺序，NAT 规则实例的标识依次为 A、B、C 、……、，可使用 **show ip nat summary**（章节 3.6.1）查看。
- AGE：该 NAT 会话的创建时间。
- Totally 91 items：当前的 NAT 会话表的表项数。

3.6.3 查看 NAT 静态映射

使用命令 **show ip nat translation static**，不仅可以查看由 NAT 静态映射产生的 NAT 会话信息，同时也可以方便的查看当前配置的所有 NAT 静态映射的相关信息。

配置命令如表 3-37 所示。

操作	命令
查看由 NAT 静态映射产生的 NAT 会话信息	**show ip nat translation static**

表 3-38 查看 NAT 静态映射

以下提供了一个使用命令“ **show ip nat translation static** ”查看全部 NAT 静态映射信息的实例。

```
hiper% show ip nat translation
NO      SrcIP       SrcPORT        DestIP   DestPORT  P  OutPkt   InPkt  GPORT  BID    AGE
1   200.200.200.15   tftp         0.0.0.0          0  U       0       0   6915   A   77562
2   200.200.200.15   telnt   61.171.252.182    16571  T   34256   44655   2023   A       1
3   200.200.200.50   3389      61.144.83.7      2596  T    3269    2517   3389   A   12186
4   200.200.200.95   5900         0.0.0.0          0  T       0       2   5900   A   77562
5   200.200.200.95   telnt        0.0.0.0          0  T       0       0   2323   A   77562
6   200.200.200.95    ftp         0.0.0.0          0  T       0       0   2121   A   77562
7   200.200.200.150 telnt         0.0.0.0          0  T       0       0   4023   A   77562
8   200.200.200.150  http    61.171.252.182    17056  T    2418    1623   8181   A    4490
9   200.200.200.150   ftp     211.141.87.35    40468  T      10      10    ftp   A   14904

    ......  ......

19 200.200.200.254  http      218.80.119.20     3536  T      32      32   8081   A   18156
Totally 19 items
```

图 3-3 查看 NAT 静态映射

图 3-3 中，各参数的涵义请参考章节 3.6.2。需要特别指出的是，NAT 静态映射的配置信息可通过查看各条目中的参数“ SrcIP ”、“ SrcPORT ”、“ DestIP ”、“ DestPORT ”、“ P ”、“ GPORT ”、“ BID ”的值获得。

此外，当某条 NAT 静态映射未被使用时，“ DestIP ”的值为 0.0.0.0，“ DestPORT ”、“ OutPkt ”以及“ InPkt ”的值都为 0。当有外部主机访问某台内部主机通过 NAT 静态映射提供的服务时，“ DestIP ”和“ DestPORT ”将分别显示为该外部主机的 IP 地址及其使用的端口。当有多台外部主机访问该服务时，系统始终显示最近那次访问的外部主机的 IP 地址及端口；而“ OutPkt ”和“ InPkt ”为所有使用该 NAT 静态映射产生的 NAT 会话转发的数据包统计。

3.6.4 局域网各主机的 NAT 统计信息的查看和清除

在 HiPER 中，可以查看局域网中各主机的 NAT 统计信息，还可清除当前动态生成的 NAT 会话的统计信息。

配置命令如表 3-39 所示。

操作	命令
查看 NAT 统计信息	**show ip nat statistics**
清除 NAT 统计信息	**clear ip nat**
备注：执行清除命令后，各主机动态生成的的 NAT 会话统计信息都将被清除。	

表 3-39 查看/清除局域网各主机的 NAT 统计信息

以下提供了一个使用命令“ **show ip nat statistics** ”查看 NAT 统计信息的实例（如图 3-4），并结合该例对相关参数进行描述和说明。

```
hiper% show ip nat statistics
 NO   IpAddress      Inuse    Used    OutPkt    InPkt     Req   Reuse     New    OverF

 1  200.200.200.50     3        3      2499      1853      20       0      20        0
 2  200.200.200.54     3        3      2085      3861       3       0       3        0
 3  200.200.200.87     3        5      3232      2396     113      12     101        0
 4  200.200.200.95     3        3         0         0       6       0       6        0
 5  218.82.48.103      5       14      1855      1825     131       4     127        0
 6  200.200.200.121    0        0       143       219       4       0       4        0
 7  200.200.200.139    3        3      1928      2068     120      17     103        0
 8  200.200.200.150    3        3        29         7      16       0      16        0
 9  200.200.200.177    1        1         0         0       2       0       2        0

  ……  ……
28 200.200.200.233    3      18     8325     9711      712      291      421       0

Totally 28 hosts
```

图 3-4 查看局域网各主机的 NAT 统计信息

图 3- 4 中，NAT 统计信息中各个参数涵义如下：

- NO：序号。
- IpAddress：局域网某用户主机的 IP 地址。
- Inuse：该用户主机当前正在使用的 NAT 会话数量。
- Used：上一次清除至查看时刻这段时间内，该用户主机使用的 NAT 会话的总数量，包括当前未使用的 NAT 会话。
- OutPkt：上一次清除至查看时刻这段时间内，该主机做 NAT 上传（发送）数据包的数量。
- InPkt：上一次清除至查看时刻这段时间内，该主机做 NAT 下载（接收）数据包的数量。
- Req：上一次清除至查看时刻这段时间内，该主机发起的 NAT 请求的总次数。
- Reuse：上一次清除至查看时刻这段时间内，该主机发起的 NAT 请求中重用已有的 NAT 会话表中的非活动项的次数。
- New：上一次清除至查看时刻这段时间内，该主机发起的 NAT 请求中新创建的 NAT 会话的次数。
- OverF：上一次清除至查看时刻这段时间内，该用户主机 NAT 请求超过 HiPER 内部限制的数量，用户最大 NAT Session 数的涵义及配置请参考章节 3.1.2。
- Totally 28 hosts：当前连接到 HiPER 做 NAT 的局域网主机的总数量。

第4章 NAT 配置实例

4.1 NAT 规则配置实例

4.1.1 EasyIP 方式应用实例

1. 需求

如图 3-5 所示，某网吧申请了 2 条线路，其中一条是联通 4M 光纤，联通分配给网吧使用的连接地址为 218.1.21.2/30，218.1.21.1/30 是该线路的网关地址。另外一条是电信的 2M ADSL 拨号上网，帐号为 ad12345678，密码为 197692，CHAP 验证方式，包月计费方式。内部网络的地址为 192.168.16.0/24。

现拟定 WAN 口接电信 4M 光纤的线路，即主线路使用固定 IP 接入方式；WAN2/DMZ 口接电信的 2M ADSL 的线路，即备份线路采用 PPPoE 拨号上网方式。

另外，要求内部机器必按照带宽来分配流量，整体使用带宽可接近 6M，并且，当其中某条线路故障时，内部机器可以自动切换到另外那条正常线路上。

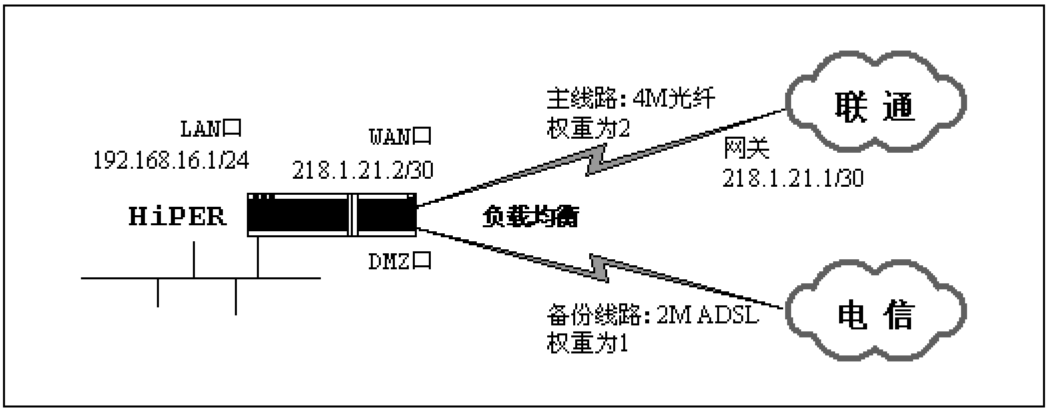

图 3-5 NAT 规则配置实例——EasyIP 方式

2. 分析

由于主线路是采用固定 IP 接入方式上网，因此首先需要指定 WAN 口的 IP 地址及子网掩码，并设置主线路的静态网关；然后再配置 PPPoE 拨号上网连接实例，由于该线路是包月计费，因此可采用自动拨号方式。因为是从 WAN2/DMZ 口拨号，因此必须启用呼叫分组功能并将 WAN2/DMZ 口的呼叫组号设为 6。

此外，还需启用 NAT 功能，并设置主线路 NAT 规则和备份线路 NAT 规则，以保证局域网用户能使用两条线路共享上网。由于要求按带宽比分配流量，整体使用带宽接近 6M，因此，两条线路必须采用相同的优先级和断开优先级（本例中使用缺省值即可），以实现负

载均衡；另外，由于两条线路的带宽比为 2∶1，因此主线路 NAT 规则和备份线路 NAT 规则的权重可分别设为 2 和 1。

最后，为保证 NAT 工作正常，还需启用快速转发功能。

3. 配置步骤

1) 配置主线路

！配置 WAN 口 IP 地址以及子网掩码（LAN 口使用缺省配置）

```
set interface ehternet/2 ip address 218.1.21.2
set interface ehternet/2 ip netmask 255.255.255.252
```

! 关闭 WAN 口自动获得地址的功能

```
set interface ehternet/2 dhcpclientpnp disabled
```

! 设置静态网关

```
set ip route static/Default gateway 218.1.21.1
```

2) 配置呼叫分组功能及呼叫组号

! 启用呼叫分组功能

```
set system dialergroup enabled
```

！设置 WAN2/DMZ 口的呼叫组号为 6

```
set interface ethernet/3 dialergroup 6
```

3) 配置备份线路

！新建一个 PPPoE 拨号连接实例，自定义连接名为 PPOE

```
new connection/PPOE
```

！设置一个首拨号码（从 DMZ 口呼出，必须以 6 开头）

```
set connection/PPOE dial first 61
```

！设置 PPP 验证方式、用户名、密码

```
set connection/PPOE encaps send authtype chap
set connection/PPOE encaps send name ad12345678
set connection/PPOE encaps send pw 197692
```

！启用 PPPoE 客户端功能

```
set connection/PPOE pppoe type client
```

！设置拨号类型为自动拨号

```
set connection/PPOE line calltype AO/Switched
set connection/PPOE line dialoutspoof yes
```

！设置空闲时间为 0（即连接空闲不断线）

```
set connection/PPPOE dial idletimeout 0
```

4) 启用 NAT 功能

！启用 NAT 功能

```
set ip nat routing enabled
```

5) 配置主线路 NAT 规则

！新建一条 NAT 规则，自定义 NAT 规则名为 ETHbind

```
new ip nat binding/ETHbind
```

! 设置主线路 NAT 规则的类型为 EasyIP

```
set ip nat binding/ETHbind natmethod easyip
```

！设置主线路 NAT 规则的绑定端口为 eth2

```
set ip nat binding/ETHbind profile eth2
```

！设置主线路 NAT 规则的权重值为 2

```
set ip nat binding/ETHbind weight 2
```

6) 配置备份线路 NAT 规则

！新建一条备份线路 NAT 规则，自定义规则名为 PBIND

```
new ip nat binding/PBIND
```

！将备份线路 NAT 规则绑定到备份线路

```
set ip nat binding/PBIND profile PPOE
```

！设置备份线路 NAT 规则的类型为 EasyIP

```
set ip nat binding/PBIND natmethod easyip
```

7) 其他配置

！启用快速转发功能

```
set system l3Switch enabled
```

8) 保存配置

! 保存配置

```
write
```

4.1.2 One2One 方式应用实例

1. 需求

如图 3-6 所示，某企业申请了一条电信的线路，固定 IP 接入方式，带宽为 6M。电信给它分配了 5 个地址：202.1.1.130/29～202.1.1.1.134/29，使用电信提供的网关 202.1.1.129/29。

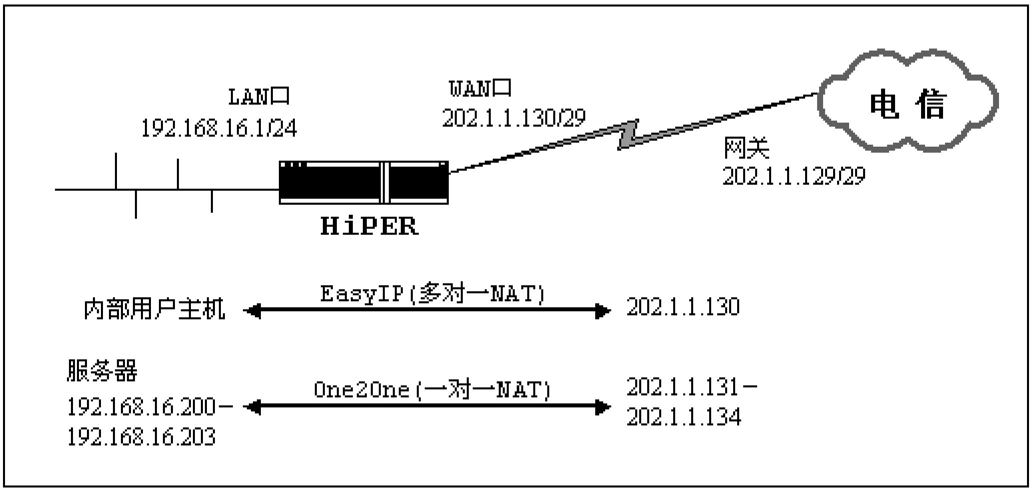

图 3-6 NAT 规则配置实例——One2One 方式

该企业希望内部的人员上网通过 NAT 后使用 202.1.1.130/29 共享上网，另外有四台服务器做一对一 NAT（One2One）使用 202.1.1.131/29～202.1.1.1.134/29 对外提供服务。内部网络的地址是 192.168.16.0/24，4 台服务器的内部地址是 192.168.16.200/24～192.168.16.203/24。

2. 分析

由于该线路是采用固定 IP 接入方式上网，因此需要指定 WAN 口的 IP 地址及其子网掩码，并设置静态网关；此外，还需启用 NAT 功能，并设置主线路 NAT 规则，以保证局域网用户能使用 WAN 口 IP 地址共享上网。

而该企业使用提供四台内部服务器供外部访问，因此还需为它们设置一个类型为“One2One”的 NAT 规则。

最后，为保证 NAT 工作正常，还需启用快速转发功能；而由于 WAN 口是多地址接入，因此还需在 WAN 口启用 NAT 类型的 ARP 代理功能；另外，如果局域网用户需要通过外部地址（202.1.1.131～202.1.1.134）访问内部服务器，还需设置相关的静态路由。

3. 配置步骤

1) 配置主线路

！配置 WAN 口 IP 地址以及子网掩码（LAN 口使用缺省配置）

```
set interface ehternet/2 ip address 202.1.1.130
set interface ehternet/2 ip netmask 255.255.255.248
```

！ 关闭 WAN 口自动获得地址的功能

```
set interface ehternet/2 dhcpclientpnp disabled
```

！ 设置静态网关

```
set ip route static/Default gateway 202.1.1.129
```

2) 启用 NAT 功能

！启用 NAT 功能

```
set ip nat routing enabled
```

3) 配置主线路 NAT 规则

！新建 NAT 规则，自定义 NAT 规则名为 ETHbind

```
new ip nat binding/ETHbind
```

！ 设置 NAT 规则的类型为 EasyIP

```
set ip nat binding/ETHbind natmethod easyip
```

！设置 NAT 规则的绑定端口为 eth2

```
set ip nat binding/ETHbind profile eth2
```

4) 配置内部服务器使用的 NAT 规则

！新建一条 NAT 规则，自定义 NAT 规则名为 example2

```
new ip nat binding/example2
```

！ 设置 NAT 规则的类型为 One2One

```
set ip nat binding/example2 natmethod one2one
```

！设置 NAT 规则的绑定端口为 eth2

```
set ip nat binding/example2 profile eth2
```

！设置该 NAT 规则的外部起始 IP 地址为 202.1.1.131

```
set ip nat binding/example2 globalip 202.1.1.131
```

！设置 NAT 规则的内部起始 IP 地址和结束 IP 地址分别为 192.168.16.200 和 192.168.16.203

```
set ip nat binding/example2 internalipfrom 192.168.16.200
set ip nat binding/example2 internalipto 192.168.16.203
```

5) 其他配置

！启用快速转发功能

```
set system l3Switch enabled
```

！在 WAN 口启用 NAT 类型的 ARP 代理功能

```
set interface ethernet/2 ip arpproxy nat
```

！局域网用户如果要访问 202.1.1.131～202.1.1.134，必须要设置相关的静态路由
！配置局域网用户访问 202.1.1.131 使用的静态路由

```
new ip route static/nat1
set ip route static/nat1 dest 202.1.1.131
set ip route static/nat1 netmask 255.255.255.255
set ip route static/nat1 gateway 202.1.1.130
```

！配置局域网用户访问 202.1.1.132 使用的静态路由

```
new ip route static/nat2
set ip route static/nat2 dest 202.1.1.132
set ip route static/nat2 netmask 255.255.255.255
set ip route static/nat2 gateway 202.1.1.130
```

！配置局域网用户访问 202.1.1.133 使用的静态路由

```
new ip route static/nat3
set ip route static/nat3 dest 202.1.1.133
set ip route static/nat3 netmask 255.255.255.255
set ip route static/nat3 gateway 202.1.1.130
```

！配置局域网用户访问 202.1.1.134 使用的静态路由

```
new ip route static/nat4
set ip route static/nat4 dest 202.1.1.134
set ip route static/nat4 netmask 255.255.255.255
set ip route static/nat4 gateway 202.1.1.130
```

6) 保存配置

！保存配置

```
write
```

4.1.3 Passthrough 方式应用实例

1. 需求

如图 3-7 所示，某企业申请了一条电信的线路，固定 IP 接入方式，带宽是 6M。电信提供给企业使用的连接地址为 202.96.97.2/30，电信使用的连接地址（即网关地址）为 202.96.97.1/30。该企业的内部用户主机将使用 202.96.97.2/30 共享上网，内部网络的地址是 192.168.16.0/24。

此外，电信还分配了一段地址给该企业使用，地址范围为 202.96.100.0/27 ~202.96.100.31/27，该企业将利用这些地址采用 Passthrough 方式配置多台服务器，对外提供服务；注意，202.96.100.0/27 和 202.96.100.31/27 分别为子网的子网号和广播地址，不可使用。

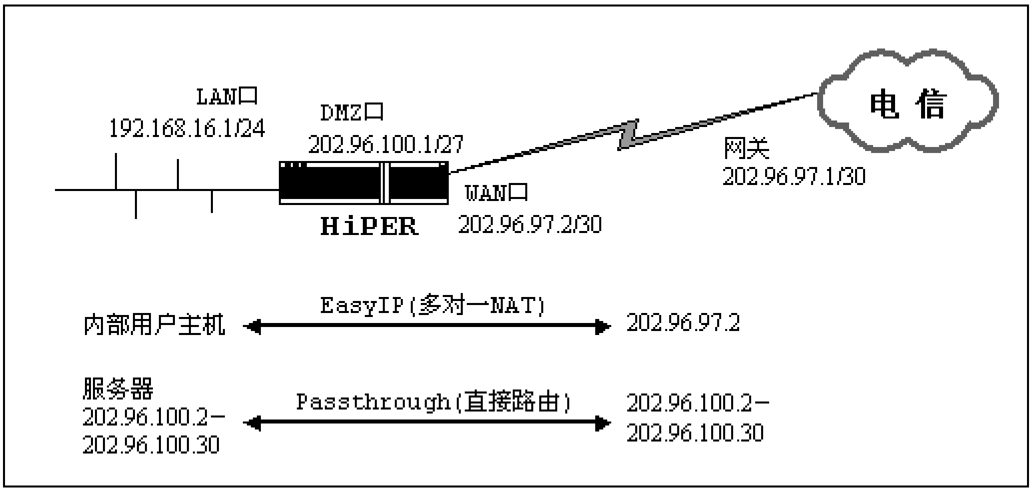

图 3-7 NAT 规则配置实例——Passthrough 方式

2. 分析

由于该线路是采用固定 IP 接入方式上网，因此需要指定 WAN 口的 IP 地址及其子网掩码，并设置静态网关；此外，还需启用 NAT 功能，并设置主线路 NAT 规则，以保证局域网用户能使用 WAN 口 IP 地址 202.96.97.2/30 共享上网。

另外，由于要求对外服务器采用 Passthrough 方式直接路由出网，因此，需将服务器通过交换机连接到 HiPER 的 WAN2/DMZ 口，将 DMZ 口的地址设为 202.96.100.1/27，并将服务器的地址设为 202.96.100.2/27~202.96.100.30/27 中的任一个，并且这些对外服务器的网关都是 202.96.100.1/27。之后，再为它们设置一个类型为“ Passthrough ”的 NAT 规则，地址范围为：202.96.100.2/27~202.96.100.30/27

最后，为保证 NAT 工作正常，还需启用快速转发功能。

3. 配置步骤

1) 配置主线路

！配置 WAN 口 IP 地址以及子网掩码（LAN 口使用缺省配置）

```
set interface ehternet/2 ip address 202.96.97.2
set interface ehternet/2 ip netmask 255.255.255.252
```

! 关闭 WAN 口自动获得地址的功能

```
set interface ehternet/2 dhcpclientpnp disabled
```

! 设置静态网关

```
set ip route static/Default gateway 202.96.97.1
```

2) 启用 NAT 功能

！启用 NAT 功能

```
set ip nat routing enabled
```

3) 配置主线路 NAT 规则

！新建 NAT 规则，自定义 NAT 规则名为 ETHbind

```
new ip nat binding/ETHbind
```

! 设置 NAT 规则的类型为 EasyIP

```
set ip nat binding/ETHbind natmethod easyip
```

！设置 NAT 规则的绑定端口为 eth2

```
set ip nat binding/ETHbind profile eth2
```

4）配置 WAN2/DMZ 口

！配置 WAN2/DMZ 口 IP 地址以及子网掩码

```
set interface ehternet/3 ip address 202.96.100.1
set interface ehternet/3 ip netmask 255.255.255.224
```

5) 配置一条类型为“ Passthrough ”的 NAT 规则，实现内部服务器直接路由上网

！新建一条 NAT 规则，自定义 NAT 规则名为 pass
```
new ip nat binding/pass
```

! 设置 NAT 规则的类型为 Passthroug
```
set ip nat binding/pass natmethod passthrough
```

！设置 NAT 规则的绑定端口为 eth2
```
set ip nat binding/pass profile eth2
```

！设置 NAT 规则的内部起始 IP 地址和结束 IP 地址分别为 202.96.100.2 和 202.96.100.30
```
set ip nat binding/example2 internalipfrom 202.96.100.2
set ip nat binding/example2 internalipto 202.96.100.30
```

6) 其他配置

！启用快速转发功能
```
set system l3Switch enabled
```

7) 保存配置

! 保存配置
```
write
```

4.2 NAT 静态映射配置实例

4.2.1 NAT 静态映射配置实例 1

1. 需求

局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，但是希望外部通过 WAN 口当前 IP 地址以及 210 端口访问这个服务。

2. 分析

由于只映射一个内部端口，因此无需设置端口范围。另外，由于是通过 WAN 口当前 IP 地址访问这个服务，因此需要将该 NAT 静态映射绑定到主线路 NAT 规则上。

3. 配置步骤

! 新建一条 NAT 静态映射，自定义其名称为 ftp
```
new ip nat static/ftp
```

! 设置 NAT 静态映射使用的协议为 TCP
```
set ip nat static/ftp protocol tcp
```

！设置 NAT 静态映射的外部端口为 210
```
set ip nat static/ftp dstport 210
```

！设置 NAT 静态映射的内部端口为 21
```
set ip nat static/ftp localport 21
```

！设置 NAT 静态映射的内部 IP 地址为 192.168.16.99
```
set ip nat static/ftp localaddress 192.168.16.99
```

！设置 NAT 静态映射绑定在主线路 NAT 规则上，这里假设规则名 ETHbind
```
set ip nat static/ftp binding ETHbind
```

！保存配置
```
write
```

4.2.2 NAT 静态映射配置实例 2

1. 需求

局域网计算机 192.168.16.100 开设了 UDP30000~UDP30019 端口的服务，希望可以映射到外部的 UDP30000~UDP30019 端口，并且希望外部是通过 WAN2/DMZ 口当前 IP 地址访问这个服务。

2. 分析

由于需映射 20 个内部端口，因此必须设置端口范围，端口范围为实际端口数量的值减去 1，即 19。另外，由于是通过 WAN2/DMZ 当前 IP 地址访问这个服务，因此需要将该 NAT 静态映射绑定到备份线路 NAT 规则上。

3. 配置步骤

！新建一条 NAT 静态映射，自定义其名称为 VOIP
```
new ip nat static/VOIP
```

！设置 NAT 静态映射使用的协议为 UDP
```
set ip nat static/VOIP protocol udp
```

！设置 NAT 静态映射的外部起始端口为 30000
```
set ip nat static/VOIP dstport 30000
```

！设置 NAT 静态映射的内部起始端口为 30000
```
set ip nat static/VOIP localport 30000
```

！设置端口范围为 19
```
set ip nat static/VOIP dstrange 19
```

！设置 NAT 静态映射的内部 IP 地址为 192.168.16.100
```
set ip nat static/VOIP localaddress 192.168.16.100
```

！设置 NAT 静态映射绑定在备份线路 NAT 规则上，这里假设规则名 IBIND
```
set ip nat static/VOIP binding IBIND
```

！保存配置
```
write
```

4.2.3 NAT 静态映射配置实例 3

1. 需求

ISP 分配了 218.1.21.0~218.1.21.7 八个地址，其中 218.1.21.1/29 是 HiPER 的网关地址，218.1.21.2/29 是 HiPER 的 WAN 口 IP 地址，局域网计算机 192.168.16.199 开设了 TCP21 端口的服务，希望外部通过 218.1.21.3 的 TCP21 端口来访问这个服务。

2. 分析

首先需配置一条类型为“ EasyIP ”的 NAT 规则，使其外部地址为 218.1.21.3，将其“ 规则名 ”设为“ example1 ”，具体配置步骤略。然后，需将 NAT 静态映射绑定到该 NAT 规则上，才能实现外部通过 218.1.21.3 来访问这个服务。

3. 配置步骤

！新建一条 NAT 静态映射，自定义其名称为 ftp2
```
new ip nat static/ftp2
```

！设置 NAT 静态映射使用的协议为 TCP
```
set ip nat static/ftp2 protocol tcp
```

！设置 NAT 静态映射的外部端口为 21
```
set ip nat static/ftp2 dstport 21
```

！设置 NAT 静态映射的内部端口为 21
```
set ip nat static/ftp2 localport 21
```

！设置 NAT 静态映射的内部 IP 地址为 192.168.16.199
```
set ip nat static/ftp2 localaddress 192.168.16.199
```

！设置 NAT 静态映射绑定在名称为“ example1 ”的规则名上
```
set ip nat static/ftp2 binding example1
```

！保存配置
```
write
```

附录一 图目录

图 1-1 网络地址转换（基本 NAT）的基本过程 3
图 1-2 网络端口地址转换（NAPT）的基本过程 4
图 3-1 查看 NAT 摘要信息 27
图 3-2 查看 NAT 会话信息 29
图 3-3 查看 NAT 静态映射 30
图 3-4 查看局域网各主机的 NAT 统计信息 31
图 3-5 NAT 规则配置实例——EasyIP 方式 32
图 3-6 NAT 规则配置实例——One2One 方式 35
图 3-7 NAT 规则配置实例——Passthrough 方式 37

附录二 表目录

表 3-1 启用/禁用 NAT 功能 12
表 3-2 设置最大 session 数 13
表 3-3 设置分配规则 13
表 3-4 新建一条 NAT 规则——EasyIP 14
表 3-5 设置 NAT 规则的类型为 EasyIP 14
表 3-6 设置 NAT 规则对应的外部 IP 地址——EasyIP 14
表 3-7 设置内部起始 IP 地址和内部结束 IP 地址——EasyIP 15
表 3-8 设置 NAT 规则的权重——EasyIP 15
表 3-9 设置 NAT 规则的绑定线路（端口）——EasyIP 15
表 3-10 启用/禁用一条 NAT 规则——EasyIP 16
表 3-11 删除一条 NAT 规则——EasyIP 16
表 3-12 新建一条 NAT 规则——One2One 17
表 3-13 设置 NAT 规则的类型为 One2One 17
表 3-14 设置 NAT 规则对应的外部起始 IP 地址——One2One 17
表 3-15 设置内部起始 IP 地址和内部结束 IP 地址——One2One 18
表 3-16 设置 NAT 规则的绑定线路（端口）——One2One 18
表 3-17 启用/禁用一条 NAT 规则——One2One 18
表 3-18 删除一条 NAT 规则——One2One 19
表 3-19 新建一条 NAT 规则——Passthrough 19
表 3-20 设置 NAT 规则的类型为 Passthrough 20
表 3-21 设置内部起始 IP 地址和内部结束 IP 地址——Passthrough 20
表 3-22 设置 NAT 规则的绑定线路（端口）——Passthrough 20
表 3-23 启用/禁用一条 NAT 规则——Passthrough 21
表 3-24 删除一条 NAT 规则——Passthrough 21
表 3-25 新建一条 NAT 静态映射 22
表 3-26 设置 NAT 静态映射的协议类型 22
表 3-27 设置 NAT 静态映射的内部 IP 地址 22
表 3-28 设置 NAT 静态映射的内部起始端口 22
表 3-29 设置 NAT 静态映射的内部起始端口 23
表 3-30 设置 NAT 静态映射的端口浮动范围 23
表 3-31 设置 NAT 静态映射所绑定的 NAT 规则 24
表 3-32 启用/禁用一条 NAT 静态映射 24
表 3-33 删除一条 NAT 静态映射 24
表 3-34 设置全局 DMZ 主机 25
表 3-35 设置局部 DMZ 主机 25
表 3-36 查看 NAT 摘要信息 27
表 3-37 查看 NAT 会话表 28
表 3-38 查看 NAT 静态映射 30

表 3-39 查看/清除局域网各主机的 NAT 统计信息 30